

1 The opinion in support of the decision being entered today was *not* written
2 for publication and is *not* binding precedent of the Board.

3
4 UNITED STATES PATENT AND TRADEMARK OFFICE

5
6
7 BEFORE THE BOARD OF PATENT APPEALS
8 AND INTERFERENCES

9
10
11 *Ex parte* CAROLYN RAMSEY CATAN

12
13
14 Appeal 2007-0820
15 Application 09/734,808
16 Technology Center 1700

17
18
19 Decided: July 3, 2007

20
21
22 Before MICHAEL R. FLEMING, *Chief Administrative Patent Judge*,
23 HUBERT C. LORIN, ALLEN R. MacDONALD, LINDA E. HORNER, and
24 ANTON W. FETTING, *Administrative Patent Judges*.

25
26 PER CURIAM

27
28
29 DECISION ON APPEAL

30
31
32 STATEMENT OF THE CASE

33
34 The appeal is from a decision of the Examiner rejecting claims 5-11
35 and 13-16¹. 35 U.S.C. § 134 (2002). We have jurisdiction under 35 U.S.C.
36 § 6(b) (2002).

¹ Claims 1-4, 12, and 17 have been canceled.

1 Claims 5-11 and 13-16 are rejected under 35 U.S.C. § 103(a) (2002)
2 over Nakano (US Patent 5,845,260) in view of Dethloff (US Patent
3 4,837,422) and Harada (US Patent 5,721,583).

4 We AFFIRM.

5 Appellant's claimed invention is a consumer electronics device using
6 bioauthentication to authorize sub-users of an authorized credit account to
7 place orders over a communication network up to a pre-set maximum sub-
8 credit limit. The device includes a bioauthentication device, such as a
9 fingerprint sensor (claim 6) or voice sensor (claim 8). The claimed
10 electronics device comprises a memory, a processor, and a communications
11 link. The memory stores account information for an account holder as well
12 as bioauthentication information and sub-credit limits for authorized users of
13 the account. The processor (a) detects a match between bioauthentication
14 information received from the bioauthentication device and
15 bioauthentication information stored in memory, and when a match is
16 detected, (b) finds a sub-credit limit associated with the bioauthentication
17 information, and when a sub-credit limit is not exceeded, (c) sends account
18 holder information over the communication link to enable the user of the
19 electronics device to place an order.

20 Appellant, in the Brief², argues claims 5-11 and 13-16 as a group.
21 The Board selects representative claim 5 to decide the appeal. 37 C.F.R.
22 § 41.37(c)(1)(vii) (2006). Accordingly, the remaining claims stand or fall
23 with claim 5.

² Our decision will make reference to Appellant's Appeal Brief ("Appeal Br.," filed Aug. 9, 2006), the Examiner's Answer ("Answer," mailed Aug. 17, 2006), and to the Reply Brief ("Reply Br.," filed Oct. 17, 2006).

1 Claim 5 reads as follows:

2 5. A consumer electronics device, comprising
3 a memory which stores account information for an account
4 holder and sub-credit limits and bioauthentication information for
5 authorized users of the account;
6 a bioauthentication device which provides bioauthentication
7 information to the memory;
8 a communication link; and
9 a processor, which compares received bioauthentication
10 information to stored bioauthentication information to detect a match,
11 and finds an associated sub-credit limit corresponding to the received
12 bioauthentication information, to enable a purchase over the response
13 network via the communication network up to a maximum of the sub-
14 credit limit, the processor sending the account holder information over
15 the communication link only if the match is detected and the sub-
16 credit limit is not exceeded.

17
18 ISSUE

19 The issue is whether Appellant has shown that the Examiner erred in
20 holding the combination of Nakano's consumer electronics device and
21 Dethloff's and Harada's bioauthentication means would have rendered the
22 subject matter of claim 5 obvious to one of ordinary skill in the art at the
23 time of the invention.

24
25 FINDINGS OF FACT

26 The record supports the following findings of fact (FF) by a
27 preponderance of the evidence.

28 1. Claim 5 does not describe the "consumer electronics device" of
29 the preamble in terms that limit any function, including the
30 steps of bioauthenticating and determining whether a sub-credit
31 limit is exceeded, to a "local" processor.

- 1 2. The words “local” or “locally” appear nowhere in the claim.
- 2 3. According to the claim, the “consumer electronics device”
- 3 *comprises* a “processor,” but the claim does not state where the
- 4 processor is located or where its functions must be performed.
- 5 4. Although a “consumer electronics device” may be a single,
- 6 unitary object, housing all the functions needed to operate the
- 7 device, that is not always the case. Consumer electronics
- 8 devices packaged to include, for example, a combination of a
- 9 base station and a remote transmitter, whereby the base station
- 10 processes information received from the remote transmitter
- 11 (e.g., by wireless communication), are also well known.
- 12 5. Claim 5 is worded broadly and thus does not exclude such a
- 13 combination.
- 14 6. Furthermore, the Specification describes, as an embodiment of
- 15 the inventive device, a system wherein the bioauthentication
- 16 and sub-credit limit matching functions reside on a server:

17 It is another object of the invention to

18 provide a method and device, which, based

19 on authentication of the user, enables the

20 owner of the account to easily delegate

21 different monetary degrees of access to the

22 owner’s single account to different people

23 and enables the entire family to access the

24 account via a bioauthentication sensor. In

25 this embodiment the account and

26 bioauthentication information is stored at a

27 server so that access to the server can be

28 achieved at home, at school, in a hotel, or

29 other remote location.

30 (Specification 2:20-3:4.)

1 7. The Specification further describes using the server as the
2 processor:

3 An authorized user then uses his PC,
4 mobile phone or television 10 to access the
5 Internet and an on-line store 11. The
6 authorized user selects an item or service for
7 purchase. The on-line store 11 requests a
8 credit card number. The bioauthentication
9 information (fingerprint, iris scan etc.) is
10 sent to the server 12. The server 12 locates
11 the correct credit card information and
12 checks whether the authorized user can
13 spend the amount requested. In one
14 embodiment, the authorized user informs the
15 server 12 of the amount to be spent and in
16 another embodiment the on-line store 11
17 gives the amount to the server. If
18 authorization is approved, the server 12
19 sends the on-line store 11 the credit card
20 information required to complete the sale.

21 (Specification 6:3-13.)

22 8. Because the scope of claim 5 is not limited to use of a “local”
23 processor, Nakano discloses all of the elements of claim 5
24 except for Nakano’s authentication information is not provided
25 by a bioauthentication device (Answer 3-5) (Appeal Br. 8-9).

26 9. The Examiner found that Harada discloses “bio-authentication
27 information as the identification information where [the]
28 bio-authentication device provides the bio-authentication
29 information that is a fingerprint (col 7, lines 19-23) further
30 where the sensor is on the remote control (col 7, lines 14-18)”
31 (Answer 6). Appellant did not traverse these findings by the
32 Examiner as to the scope and content of Harada (Appeal Br. 10-

1 11 and 17-18). Thus, Harada shows that the use of a
2 bioauthentication device (fingerprint sensor) on a consumer
3 electronics device (remote control) to provide bioauthentication
4 information (fingerprint) was known in the prior art at the time
5 of the invention.

6 10. Harada teaches to use bioauthentication information, such as a
7 voice print or fingerprint, “to prevent unauthorized tampering
8 with [certain terminal setting] data by persons who may have
9 access to the remote control apparatus” (Harada, col. 4, ll. 32-
10 34), “to ensure that the type of service which is provided by a
11 terminal apparatus to the users of its remote control apparatuses
12 is selectively controlled in accordance with various different
13 categories of uses, e.g.,] adults and children” (Harada, col. 4,
14 ll. 56-60), and “to reliably ensure that certain services which
15 should be available only to a specific individual user ... and
16 which can be requested by operation of a remote control
17 apparatus, will in fact be made available only to the appropriate
18 individual, when a number of different individuals can use
19 remote control apparatus to communicate with that same
20 terminal apparatus” (Harada, col. 4, l. 61 – col. 5, l. 3).

21 11. What is clear from Harada is that the use of a PIN code is not as
22 reliable an identifier as bioauthentication information because
23 the PIN can be stolen and used without the authorized user’s
24 knowledge by anyone who may have access to the remote
25 control apparatus.

12. Harada suggests that bioauthentication information, such as a fingerprint, unambiguously and reliably ensures that a specific authorized user is requesting the service.
13. We further note that use of a PIN code as an identifier is not as desirable as bioauthentication information because the use of a PIN requires the user to remember the PIN code.
14. Dethloff is directed to “plastic devices, comprising integrated circuits, commonly called ‘smart cards’” (Dethloff, col. 1, ll. 12-18).
15. Dethloff is specifically directed to modules or “M-cards” which comprise a keyboard for entering, for example, identification and transaction data, a memory for storing data, a logic means, and a display (Dethloff, col. 9, ll. 57-68).
16. Dethloff’s M-card contains means to assign the card to a number of sub-users (Dethloff, col. 5, ll. 19-20), each of which can be designated a particular value (Dethloff, col. 5, ll. 20-28). This is accomplished by the card-holder assigning each sub-user a PIN and a transaction limit (see, e.g., Dethloff, col. 6, ll. 64- col. 7, l. 4; Fig. 9), which are stored in a memory means in the card (PIN: Dethloff, col. 11, l. 10; transaction limit: Dethloff, col. 13, ll. 17-21).
17. In operation, a sub-user will authenticate the M-card by inputting a PIN which the card then internally checks for correctness (Dethloff, col. 10, ll. 63-67; see also col. 13, ll. 35-38). This then triggers a means within the card to open a transaction account assigned to the sub-user (Dethloff, col. 12,

1 ll. 62-64) permitting the sub-user to conduct transactions up to
2 the maximum sub-user transaction amount (Dethloff, col. 13, ll.
3 19-21).

4 18. Dethloff states that instead of a PIN, a voice print (a type of
5 bioauthentication) may be used as the sub-user enabling code:

6 It is noted that while the PIN is given
7 as an example of cardholder and sub-user
8 enabling code, any other code can be used,
9 such as a voice print (to be stored as data
10 and input by the cardholder or sub-user) . . .

11 (Dethloff, col. 11, ll. 26-29.) Thus, Dethloff explicitly shows
12 that the substitution of alternative user authentication
13 techniques is known in the prior art. In particular, Dethloff
14 teaches that it was known in the art at the time of the invention
15 to substitute a PIN authentication with bioauthentication to
16 enable a user to access credit.

17 19. The art of consumer electronics devices evidences a common
18 usage of personal codes or personal identification numbers
19 (PINs) to identify or authenticate users (e.g., Nakano, col. 4,
20 ll. 42-45 and col. 5, ll. 39-42 and Dethloff, col. 10, ll. 59-67).

21 20. The art further shows that one of ordinary skill in the consumer
22 electronic device art at the time of the invention would have
23 been familiar with using bioauthentication information
24 interchangeably with or in lieu of PINs to authenticate users
25 (Harada, col. 7, ll. 14-23 and Dethloff, col. 11, ll. 26-29.)

26 21. It is also clear from an examination of the prior art that those of
27 ordinary skill in the consumer electronic device art at the time

1 of the invention were familiar with the use of bioauthentication
2 devices to obtain bioauthentication information to identify users
3 (Harada, col. 7, ll. 14-23).
4

5 PRINCIPLES OF LAW

6 “Section 103 forbids issuance of a patent when ‘the differences
7 between the subject matter sought to be patented and the prior art are such
8 that the subject matter as a whole would have been obvious at the time the
9 invention was made to a person having ordinary skill in the art to which said
10 subject matter pertains.’” *KSR Int’l Co. v. Teleflex Inc.*, 127 S.Ct. 1727,
11 1734, 82 USPQ2d 1385, 1391 (2007). The question of obviousness is
12 resolved on the basis of underlying factual determinations including (1) the
13 scope and content of the prior art, (2) any differences between the claimed
14 subject matter and the prior art, (3) the level of skill in the art. *Graham v.*
15 *John Deere Co.*, 383 U.S. 1, 17-18, 148 USPQ 459, 467 (1966). *See also*
16 *KSR*, 127 S.Ct. at 1734, 82 USPQ2d at 1391 (“While the sequence of these
17 questions might be reordered in any particular case, the [*Graham*] factors
18 continue to define the inquiry that controls.”) The Court in *Graham* further
19 noted that evidence of secondary considerations, such as commercial
20 success, long felt but unsolved needs, failure of others, etc., “might be
21 utilized to give light to the circumstances surrounding the origin of the
22 subject matter sought to be patented.” 383 U.S. at 18, 148 USPQ at 467.
23

24 In *KSR*, the Supreme Court emphasized “the need for caution in
25 granting a patent based on the combination of elements found in the prior
26 art,” *id.* at 1739, 82 USPQ2d at 1395, and discussed circumstances in which

1 a patent might be determined to be obvious without an explicit application of
2 the teaching, suggestion, motivation test.

3 In particular, the Supreme Court emphasized that “the principles laid
4 down in *Graham* reaffirmed the ‘functional approach’ of *Hotchkiss*, 11
5 How. 248.” *KSR*, 127 S.Ct. at 1739, 82 USPQ2d at 1395 (citing *Graham v.*
6 *John Deere Co.*, 383 U.S. 1, 12, 148 USPQ 459, 464 (1966) (emphasis
7 added)), and reaffirmed principles based on its precedent that “[t]he
8 combination of familiar elements according to known methods is likely to be
9 obvious when it does no more than yield predictable results.” *Id.* The Court
10 explained:

11 When a work is available in one field of endeavor,
12 design incentives and other market forces can
13 prompt variations of it, either in the same field or a
14 different one. If a person of ordinary skill can
15 implement a predictable variation, §103 likely bars
16 its patentability. For the same reason, if a
17 technique has been used to improve one device,
18 and a person of ordinary skill in the art would
19 recognize that it would improve similar devices in
20 the same way, using the technique is obvious
21 unless its actual application is beyond his or her
22 skill.

23 *Id.* at 1740, 82 USPQ2d at 1396. The operative question in this “functional
24 approach” is thus “whether the improvement is more than the predictable use
25 of prior art elements according to their established functions.” *Id.*

26 The Supreme Court made clear that “[f]ollowing these principles may
27 be more difficult in other cases than it is here because the claimed subject
28 matter may involve more than the simple substitution of one known element
29 for another or the mere application of a known technique to a piece of prior
30 art ready for the improvement.” *Id.* The Court explained, “[o]ften, it will be

1 necessary for a court to look to interrelated teachings of multiple patents; the
2 effects of demands known to the design community or present in the
3 marketplace; and the background knowledge possessed by a person having
4 ordinary skill in the art, all in order to determine whether there was an
5 apparent reason to combine the known elements in the fashion claimed by
6 the patent at issue.” *Id.* at 1740-41, 82 USPQ2d at 1396. The Court noted
7 that “[t]o facilitate review, this analysis should be made explicit. *Id.* (citing
8 *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006))
9 (“[R]ejections on obviousness grounds cannot be sustained by mere
10 conclusory statements; instead, there must be some articulated reasoning
11 with some rational underpinning to support the legal conclusion of
12 obviousness”). However, “the analysis need not seek out precise teachings
13 directed to the specific subject matter of the challenged claim, for a court can
14 take account of the inferences and creative steps that a person of ordinary
15 skill in the art would employ.” *Id.* at 1741, 82 USPQ2d at 1396.

16 The Supreme Court’s opinion in *United States v. Adams*, 383 U.S. 39,
17 40, 148 USPQ 479, 480 (1966) is illustrative of the “functional approach” to
18 be taken in cases where the claimed invention is a prior art structure altered
19 by substituting one element in the structure for another known element.
20 *KSR*, 127 S.Ct. at 1734, 82 USPQ2d at 1391. “The Court [in *Adams*]
21 recognized that when a patent claims a structure already known in the prior
22 art that is altered by the mere substitution of one element for another known
23 in the field, the combination must do more than yield a predictable result.
24 383 U.S., at 50-51.” *Id.* Ultimately the *Adams* Court found the combination
25 at issue *not* obvious to those skilled in the art because, although the elements
26 were known in the prior art, they worked together in an *unexpected* manner.

1 The [*Adams*] Court relied upon the corollary principle that when the
2 prior art teaches away from combining certain known elements,
3 discovery of a successful means of combining them is more likely to
4 be nonobvious. *Id.*, at 51-52, 86 S.Ct. 708. When Adams designed
5 his battery, the prior art warned that risks were involved in using the
6 types of electrodes he employed. *The fact that the elements worked*
7 *together in an unexpected and fruitful manner supported the*
8 *conclusion that Adams's design was not obvious to those skilled in the*
9 *art.*

10 *KSR*, 127 S.Ct. at 1740, 82 USPQ2d at 1395 (emphasis added).

11 The Federal Circuit recently concluded that it would have been
12 obvious to combine (1) a mechanical device for actuating a phonograph to
13 play back sounds associated with a letter in a word on a puzzle piece with
14 (2) an electronic, processor-driven device capable of playing the sound
15 associated with a first letter of a word in a book. *Leapfrog Ent., Inc. v.*
16 *Fisher-Price, Inc.*, 485 F.3d 1157, 1161, 82 USPQ2d 1687, 1690-91 (Fed.
17 Cir. 2007) (“[a]ccommodating a prior art mechanical device that
18 accomplishes [a desired] goal to modern electronics would have been
19 reasonably obvious to one of ordinary skill in designing children’s learning
20 devices”). In reaching that conclusion, the Federal Circuit recognized that
21 “[a]n obviousness determine is not the result of a rigid formula disassociated
22 from the consideration of the facts of a case. Indeed, the common sense of
23 those skilled in the art demonstrates why some combinations would have
24 been obvious where others would not.” *Id.* at 1161, 82 USPQ2d at 1687
25 (citing *KSR*, 127 S.Ct. 1727, 1739, 82 USPQ2d 1385, 1395 (2007) (“The
26 combination of familiar elements according to known methods is likely to be
27 obvious when it does no more than yield predictable results.”). The Federal
28 Circuit relied in part on the fact that Leapfrog had presented no evidence that
29 the inclusion of a reader in the combined device was “uniquely challenging

1 or difficult for one of ordinary skill in the art” or “represented an unobvious
2 step over the prior art.” *Id.* (citing *KSR*, 127 S.Ct. at 1740-41, 82 USPQ2d at
3 1396).

4 The person of ordinary skill in the art is a hypothetical person who is
5 presumed to know the relevant prior art. *Custom Accessories, Inc. v. Jeffrey-*
6 *Allan Indus., Inc.*, 807 F.2d 955, 962, 1 USPQ2d 1196, 1201 (Fed. Cir.
7 1986). In determining this skill level, the court may consider various
8 factors including “type of problems encountered in the art; prior art solutions
9 to those problems; rapidity with which innovations are made; sophistication
10 of the technology; and educational level of active workers in the field.” *Id.*
11 (cited in *In re GPAC*, 57 F.3d 1573, 1579, 35 USPQ2d 1116, 1121 (Fed. Cir.
12 1995)). In a given case, every factor may not be present, and one or more
13 factors may predominate. *Id.* at 962-63, 1 USPQ2d at 1201.

14 ANALYSIS

15 *Claim Interpretation*

16 Appellant argues that claim 5 should be limited to a “local” processor.
17 Claims are given their broadest reasonable construction “in light of the
18 specification as it would be interpreted by one of ordinary skill in the art.”
19 *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364, 70 USPQ2d 1827,
20 1830 (Fed. Cir. 2004). Claim 5 does not describe the device in terms that
21 limit any function, including the steps of bioauthenticating and determining
22 whether a sub-credit limit is exceeded, to a “local” processor (FF 1). In fact,
23 the words “local” or “locally” appear nowhere in the claim (FF 2). The only
24 recitation in the claim relevant to the question of where the processor and its
25 recited functions may be located in the claimed device is in the preamble,
26

1 i.e., in the phrase “consumer electronics device” itself. According to the
2 claim, the “consumer electronics device” *comprises* a “processor” but it does
3 not say where the processor is located or where its functions must be
4 performed (FF 3). Although a “consumer electronics device” may be a
5 single, unitary object, housing all the functions needed to operate the device,
6 that is not always the case. Consumer electronics devices packaged to
7 include, for example, a combination of a base station and a remote
8 transmitter whereby the base station processes information received from the
9 remote transmitter (e.g., by wireless communication) are also well known
10 (FF 4). The claim is worded broadly and thus does not exclude such a
11 combination (FF 5). Furthermore, the Specification describes, as an
12 embodiment of the inventive device, a system wherein the bioauthentication
13 and sub-credit limit matching functions reside on a server (FF 6, 7). In light
14 of the Specification, the claimed “device” has a broad scope and does not
15 limit the processor to one that is “locally” positioned.

16
17 *The Graham Factors*

18 The patentability of claim 5 under 35 U.S.C. § 103(a) (2002) depends
19 on whether the claimed subject matter is obvious in view of Nakano,
20 Dethloff, and Harada.

21 The Examiner found that Nakano discloses all of the elements of
22 claim 5 except for Nakano’s authentication information is not provided by a
23 bioauthentication device, and Nakano fails to disclose a local storage device
24 for the memory, where the memory is part of the consumer electronics
25 device (Answer 4-5). The Appellant does not traverse these findings by the
26 Examiner (Appeal Br. 8-9). We disagree, however, with the Examiner’s

1 implied finding that claim 5 requires the memory to be stored in a local
2 storage device, as discussed *supra*. Accordingly, we disagree with
3 Appellant's argument that the claimed device distinguishes over Nakano
4 because Nakano determines whether a sub-credit limit is exceeded at a
5 remote server rather than "locally." Thus, the sole difference between
6 Nakano and the subject matter of claim 5 is that Nakano does not disclose
7 the authentication information being provided by a bioauthentication device
8 (FF 8).

9 The Examiner found that Harada discloses "bio-authentication
10 information as the identification information where [the] bio-authentication
11 device provides the bio-authentication information that is a fingerprint
12 (col 7, lines 19-23) further where the sensor is on the remote control (col 7,
13 lines 14-18)" (Answer 6). Appellant did not traverse these findings by the
14 Examiner as to the scope and content of Harada (Appeal Br. 10-11 and
15 17-18). Thus, Harada shows that the use of a bioauthentication device
16 (fingerprint sensor) on a consumer electronics device (remote control) to
17 provide bioauthentication information (fingerprint) was known in the prior
18 art at the time of the invention (FF 9).

19 Because Nakano teaches every element of the device of claim 5 but
20 for the bioauthentication device element, the sole difference between
21 Appellant's claim 5 and the teachings of Nakano is the use of
22 bioauthentication in place of Nakano's password authentication (FF 8). In
23 that regard, Harada shows that it was known in the art at the time of the
24 invention to use a bioauthentication device on a remote control to provide
25 the bioauthentication information (FF 9).

26 With regard to Dethloff, the Examiner found:

1 Dethloff et al discloses bio-authentication
2 information as the identification information
3 further as a voice sensor (col 11, lines 25-30), a
4 local storage device for the memory further where
5 the memory is part of the consumer electronics
6 device (col 11, lines 2-24), sending account holder
7 information over the communication link, a match
8 detected and determining a sub-credit limit that is
9 not exceeded (col 13, lines 67-68; col 14,
10 lines 1-8).

11 (Answer 5.) We agree with the Examiner that Dethloff discloses that instead
12 of using a PIN for authentication, a voice print (a type of bioauthentication)
13 may be used as the sub-user enabling code (FF 18). As such, Dethloff
14 teaches that it was known in the art at the time of the invention to substitute
15 a PIN authentication with bioauthentication to enable a user to access credit
16 via a consumer electronics device (FF 18).

17 We find, based on our examination of the prior art and the state of the
18 art in consumer electronic devices, that the art evidences a common usage of
19 personal codes or personal identification numbers (PINs) to identify or
20 authenticate users (FF 19). The art further shows that one of ordinary skill
21 in the consumer electronic device art at the time of the invention would have
22 been familiar with using bioauthentication information interchangeably with
23 or in lieu of PINs to authenticate users (FF 20). It is also clear from an
24 examination of the prior art that those of ordinary skill in the consumer
25 electronic device art at the time of the invention would have been familiar
26 with using bioauthentication devices to obtain bioauthentication information
27 to identify users (FF 21).

28
29 *Obviousness*

1 Based on an analysis of the scope and content of Nakano and Harada,
2 the facts support the conclusion that, but for the bioauthentication means,
3 Nakano discloses all the elements of the claimed device and their functions
4 and that the bioauthentication means was disclosed in Harada. Since each
5 individual element and its function, as described in claim 5, are shown in the
6 prior art, albeit shown in separate references, the difference between the
7 claimed subject matter and that of the prior art rests not on any individual
8 element or function but in the very combination itself; that is, in the
9 substitution of Harada's bioauthentication device for Nakano's manual
10 authentication means. Where, as here "[an application] claims a structure
11 already known in the prior art that is altered by the mere substitution of one
12 element for another known in the field, the combination must do more than
13 yield a predictable result," *KSR*, 127 S.Ct. at 1740, 82 USPQ2d at 1395
14 (citing *United States v. Adams*, 383 U.S. 50-51, 148 USPQ 479, 483 (1966)).
15 In that regard, Appellant has provided no evidence that replacing Nakano's
16 manual authentication means with Harada's known bioauthentication means
17 yields an unexpected result or was beyond the skill of one having ordinary
18 skill in the art.

19 The Appellant's own Specification only generally describes the idea
20 of incorporating a bioauthentication device, such as a fingerprint sensor, into
21 a consumer electronics device and the matching function needed to compare
22 the scanned bioauthentication information with the stored bioauthentication
23 information (e.g., Specification 6:6-7 and 6:17-7:2). The Specification does
24 not provide a detailed description of the implementation in hardware or
25 software of the bioauthentication device. Furthermore, Appellant's
26 Specification as well as Appellant's arguments do not present any evidence

1 that including the bioauthentication device into the consumer electronic
2 device was uniquely challenging or difficult for one of ordinary skill in the
3 art.

4 As in *Leapfrog*, the device defined by claim 5 is an adaptation of an
5 old invention (Nakano) using newer technology that is commonly available
6 and understood in the art (Harada). Adding bioauthentication to the Nakano
7 device does no more to Nakano's device than it would do if it were added to
8 any other device. The function remains the same. Predictably,
9 bioauthentication adds greater security and reliability to an authorization
10 process (FF 12). This variation on Nakano's device, whereby the manual
11 authentication means of the Nakano device is replaced with Harada's
12 bioauthentication means, appears to present no unexpected technological
13 advance in the art. One of ordinary skill in the art of consumer electronic
14 devices would have found it obvious to update the Nakano device with the
15 modern authentication components of the Harada bioauthentication means
16 and thereby gaining, predictably, the commonly understood benefits of such
17 adaptation, that is, a secure and reliable authentication procedure (FF 12).

18 Appellant argues that the Examiner has failed to provide sufficient
19 reasoning to reach a conclusion of obviousness based on the prior art
20 (Appeal Br. 11-20). Appellant repeatedly argues for application of the
21 teaching, suggestion, motivation (TSM) test, stating that "[t]here must be
22 some suggestion or motivation, either in the references themselves, or in the
23 knowledge generally available to one of ordinary skill in the art, to modify a
24 reference or to combine reference teachings" (e.g., Appeal Br. 11). The
25 Supreme Court noted in *KSR* that although the TSM test "captured a helpful
26 insight," an obviousness analysis "need not seek out precise teachings

1 directed to the specific subject matter of the challenged claim, for a court can
2 take account of the inferences and creative steps that a person of ordinary
3 skill in the art would employ.” 127 S.Ct. at 1741, 82 USPQ2d at 1396.

4 The claim is to a structure already known in the prior art that is altered
5 by the mere substitution of one known element for another element known
6 in the field for the same function. The facts themselves show that there is no
7 difference between the claimed subject matter and the prior art but for the
8 combination itself. “[T]he mere existence of differences between the prior
9 art and an invention does not establish the invention's nonobviousness. The
10 gap between the prior art and respondent's system is simply not so great as to
11 render the system nonobvious to one reasonably skilled in the art.” *Dann v.*
12 *Johnston*, 425 U.S. 219, 230, 189 USPQ 257, 261 (1976) (holding that
13 claims directed to a machine system for automatic record keeping of bank
14 checks and deposits were obvious in view of the use of data processing
15 equipment and computer programs in the banking industry at the time of the
16 invention in combination with a prior art automatic data processing system
17 using a programmed digital computer for use in a large business
18 organization). Appellant has presented no evidence that combining the
19 Nakano device with the Harada bioauthentication means would have
20 required anything more from one of ordinary skill in the art than to
21 substitute one authentication means for a more advanced one. Accordingly,
22 we hold that the subject matter of claim 5 would have been obvious to one of
23 ordinary skill in the art given the teachings of Nakano and Harada.

24 Nonetheless, our holding is further buttressed by the teaching in
25 Dethoff of the substitutability of a voice print authentication for a PIN
26 authentication (FF 10). In particular, Dethloff teaches that it was known in

1 the art at the time of the invention to substitute a PIN authentication with
2 bioauthentication to enable a user to access credit (FF 10, 20).

3 Further, Harada provides sufficient motivation for one skilled in the
4 art to use this bioauthentication information, such as a voice print or
5 fingerprint, in lieu of a PIN in order “to prevent unauthorized tampering with
6 [certain terminal setting] data by persons who may have access to the remote
7 control apparatus,” “to ensure that the type of service which is provided by a
8 terminal apparatus to the users of its remote control apparatuses is
9 selectively controlled in accordance with various different categories of
10 uses, e.g.[,] adults and children,” and “to reliably ensure that certain services
11 which should be available only to a specific individual user ... and which
12 can be requested by operation of a remote control apparatus, will in fact be
13 made available only to the appropriate individual, when a number of
14 different individuals can use remote control apparatus to communicate with
15 that same terminal apparatus” (FF 10). The use of a PIN code is not as
16 reliable an identifier as bioauthentication information because the PIN can
17 be stolen and used without the authorized user’s knowledge (FF 11). On the
18 contrary, bioauthentication information, such as a fingerprint,
19 unambiguously and reliably ensures that a specific authorized user is
20 requesting the service (FF12). Further, use of a PIN code as an identifier is
21 not as desirable as bioauthentication information because the use of a PIN
22 requires the user to remember the PIN code (FF 13).

23 Thus, one of ordinary skill in the art would have been motivated to
24 combine the bioauthentication device of Harada with the system of Nakano
25 because Dethloff teaches that one can substitute bioauthentication
26 information for PIN information, and Harada teaches that it was a common

1 problem at the time of the invention to create a remote control that would
2 reliably ensure that the appropriate person was given access to the system.
3 The use of a fingerprint scanner, such as disclosed in Harada, was an
4 obvious solution to provide a more reliable means of identification than the
5 PIN code of Nakano. *KSR*, 127 S.Ct. at 1742, 82 USPQ2d at 1397 (“[o]ne
6 of the ways in which a patent's subject matter can be proved obvious is by
7 noting that there existed at the time of invention a known problem for which
8 there was an obvious solution encompassed by the patent's claims.”) As
9 such, we sustain the Examiner’s rejection of claims 5-11 and 13-16 as
10 unpatentable over Nakano, Harada, and Dethloff.

11
12 **CONCLUSION OF LAW**

13 On the record before us, Appellant has failed to show that the
14 Examiner erred in rejecting the claims over the prior art.

15
16 **DECISION**

17 The decision of the Examiner to reject of claims 5-11 and 13-16 under
18 35 U.S.C. § 103(a) as obvious over Nakano, Harada, and Dethloff is
19 affirmed.

20
21 No time period for taking any subsequent action in connection with
22 this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

23 **AFFIRMED**
24
25
26

Appeal 2007-0820
Application 09/734,808

1

2

3

4

5

6 hh

7

8 PHILIPS INTELLECTUAL PROPERTY & STANDARDS

9 P.O. BOX 3001

10 BRIARCLIFF MANOR, NY 10510